APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-CCS-RP-001-10
Approved: IT Policy & Planning Committee July 30, 2010
APTA Control and Communications Working Group

Securing Control and Communications Systems in Transit Environments

Part 1: Elements, Organization and Risk Assessment/Management

Previously numbered as APTA-RP-CCS-1-RT-001-10
Abstract: This document covers recommended practices for securing control and communications systems in transit environments.

Keywords: control and communications security, cyber-security, radio, SCADA, train control

Summary: This *Recommended Practice* addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk.

Scope and purpose: This document addresses the security of the following passenger rail and/or bus systems: SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location (AVL), physical security feeds (CCTV, access control), public information systems, public address systems, and radio/wireless/related communication. In the event that security/safety or other standards exist for any of the above systems, this *Recommended Practice* will supplement, provide additional guidance for, or provide guidance on how control systems may securely interface with these systems. While the agency's network infrastructure may be used for multiple purposes, this *Recommended Practice* includes protection of any control information that is communicated across the agency's network.

Passenger transit agencies and the vendor community now evolve their security requirements and system security features independently for most of the systems listed above. The purpose of this *Recommended Practice* is to share transit agency best practices; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Control and Communications Security Working Group**, which provided the primary effort in the drafting of this *Recommended Practice*.

At the time this standard was completed, the working group included the following members:

David Teumim, Chair
John Moore, Secretary
David Trimble, Editor

Carl Buck
Syed Ali
J.P. Singh
John Weikel
Leonid Bukhin
Mark Curry
Paul Muldoon
Robert Evans
Dennis Clarkson
Daniel Mondesir
Jim Giardini
Dave Bauchert
Sreeram Reddy
Steve Tom
Edwin Michie
Diane Muir
Ed McDonald
Martin Glebe
Sheri Dougherty
Mark Hartong
Pete Kofod

APTA IT Standards project team:

Martin Schroeder, APTA Chief Engineer and Senior Staff Advisor

Contents

1. Introduction

The intent of this document is to provide guidance to transit agencies on securing control and communications systems for their environments. This *Recommended Practice* spearheads an effort within APTA to extend security best practices to the transit industry.

This document provides an introductory level of understanding of this field. Subsequent parts of this document will address the specifics of equipment implementation, such as describing the different types of firewalls or intrusion detection systems and mitigation measures. It represents the contribution of "leading edge" information from transit agencies that already have a control security program, and will serve as a guide for other transit agencies to develop such a program.

This *Recommended Practice* supplements existing standards and regulations, especially as concerns vital or other life-safety systems, and is not intended to supplant them. This document is instead intended to provide an overview of the needs in cyber protection and to identify potential gaps in the current standards and regulations.

Due to the comprehensive amount of information to be conveyed, this *Recommended Practice* is divided into two parts:

- **Part 1:** Elements, Organization and Risk Assessment/Management
- **Part 2:** Security Plan Development, Execution and Maintenance

This division of text material parallels the progression of recommended steps a transit agency would follow to develop and implement a control and communications security program.

Part 1 (the subject of this document) addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communications systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting risk assessment and managing risk.

Part 2 (contained under a separate cover) will assume that the agency has completed the risk assessment and risk management steps of Part 1, and will cover how to create the security plan with security controls/countermeasures, how to implement the security plan, and how to maintain the security plan. The last section covers continuity of operations/disaster recovery.

A resource of follow-up references and sources is given at the end of Section 4.

1.1 Overview

Since the Sept. 11 attack, the use of control and communications security has grown in industry sectors such as electric power, oil and gas, and chemicals. Within the transit industry, as with other sectors, there is a movement to use commercial off-the-shelf (COTS) hardware, software and networking components such as those used in everyday business and consumer information technology (IT) systems. Such COTS systems can provide a lower total cost of ownership through lower purchase price, greater compatibility with transit business systems, and less training needed compared with older more proprietary systems. However, such systems also come with an elevated risk of computer worms, viruses and hack attacks.

Cyber attacks on rail have already been publicly documented, including the CSX railway virus attack in 2003 and the Polish tram hack in 2007. The CSX virus attack caused a morning shutdown of CSX's signaling and dispatch systems in 23 states east of the Mississippi, also halting Amtrak trains in that area. The Polish tram hack caused injury to 12 people, and derailment and damage to four vehicles. More details of these attacks

and their consequences, and details of cyber attacks affecting other industry sectors, may be found in Appendix A.

The IT groups of transit agencies and other industry sectors have used business and financial cyber security knowledge developed over the past 40 years to protect their systems. The field of control and communications security takes this IT cyber security body of knowledge and applies it along with elements of physical and personnel security to transit.

It should be noted that a successful control and communications security program represents the combined effort and cooperation of many departments within an agency, such as systems engineering, signaling, IT, human resources (HR) and facility security.

2. Transit systems elements

2.1 Introduction

The purpose of typical transit control and communications systems is to facilitate the monitoring, control and data collection of multiple types of equipment. Equipment monitored by a transit control center may include a large number of functions, such as vehicle control and scheduling, power control, ventilation control, pump monitoring, intrusion detection, etc.

In order to meet this objective, the control and communications would combine the monitoring and control functionality into one or more systems. Systems typically found in a transit environment may include train control, vehicle monitoring, traction power, ventilation control, SCADA, fare collection, closed-circuit television (CCTV), fiber optic management and various other types of communications systems.

The security requirements of control and communications will vary depending on the type of equipment being controlled, as well as the actual system infrastructure. For this reason, the security team will look at systems, equipment and functionality in order to determine the security boundaries that may be required.

Hence, this section identifies both systems and functional connectivity between systems and equipment in order to determine where security issues exist. This is extremely important when dealing with cyber security.

In an attempt to cover all issues related to transit control and communications systems, this document addresses both older and newer technologies, including standalone and legacy systems. Many of the security issues with any of these systems are very similar. Therefore, this document does not need to address all systems that may be included in a transit environment but rather addresses the common systems found, independent of the size of the transit system.

This section provides a description of the different systems that may be found in a typical transit control center. A typical system would include five main components:

- the head-end equipment, including the primary and backup control center;
- the field or slave equipment;
- the transmission media between the head-end and slave equipment ;
- the system networks connecting the head-end components together; and
- the system networks connecting the field components together.

2.2 Equipment types

Typical transit control and communications systems include different generations of equipment. In order to understand the security level required for each type of system, this *Recommended Practice* has categorized the systems into two types:

- **Legacy or closed systems.** These are non-computer type systems or standalone systems that may or may not be processor based but are not accessible externally by any means, including laptop, network and peripheral devices. These systems require physical and administrative security.
- **Advanced technology.** These are computer-based systems that may have remote connectivity (dial-up, Internet connection, etc.). They may be standalone systems or have some level of integration with other systems in the control center, and they may include connections to other systems or agencies outside of the control center. These systems require physical, administrative and cyber security.

  NOTE: The level of connectivity to other systems will play a major role in determining the cyber-security requirements needed.

2.3 Systems description

Operational needs in transit environments demand the installation of control systems in order to provide central control and monitoring of many aspects of the transit network. Some control systems provide a specific function, such as train control, vehicle monitoring or security systems, while other control systems integrate a number of different functions into one or more enhanced systems. This section categorizes control systems by their common designations, while in Section 2.4 they are categorized by the functions they perform.

2.3.1 Control systems (train control or SCADA)

Train control

Train control systems (TCS) provide automatic train supervision (ATS) and may include control capabilities to the control center. Train control systems may also provide automatic train protection (ATP) and automatic train operation (ATO) for train safety, control of train movements and directing train operations on the main line and in the yards.

Generally the field control equipment contains the vital logic controls, whereas the central office equipment monitors the rail system, providing the train controllers with the ability to manage train movement and schedules. The transmission media includes data paths among the system components.

Computer-based train control systems typically utilize one or more main servers operating on a real-time-based operating system. The network would be deemed extremely critical due to the functionality available to the applications.

A typical TCS may be designed as a completely segregated/autonomous network; however, interaction with other applications may require external connectivity. This connection to other networks should be secured in accordance with Section 5 in Part 2 of this *Recommended Practice*. This would include the use of intrusion detection systems (IDS) and firewalls at the boundaries and other network perimeter devices to secure the TCS network. Special precautions need to be taken if connectivity to Internet, Intranet or Extranet is allowed.

Supervisory control and data acquisition (SCADA) systems

SCADA systems used in the transit environment usually refer to systems that provide the remote control and monitoring of field equipment located in the rapid transit passenger stations, power substations and other miscellaneous buildings in the transit environment. Depending on the transit system infrastructure, the SCADA systems may include control and monitoring of a variety of different equipment. In some rail systems, the train control systems also include SCADA functionality. SCADA system functions usually include control of traction power, control of emergency ventilation systems and monitoring of drainage pumps and various equipment alarms, including intrusion monitoring of remote locations.

2.3.2 Communications systems

Communications systems in the transit environment typically include systems such as but not limited to radio, CCTV, intercom, public address, security, and copper and fiber optic data transmission systems. The systems may be standalone or integrated with one or more other systems, depending on the operational needs of each transit system.

2.3.3 Security control (CCTV, intrusion detection, fire systems, access control)

CCTV

Closed-circuit television systems provide a means of surveillance of passenger stations and other areas where deemed necessary. Many CCTV systems are integrated with physical intrusion detection and intercom systems. Implementation of pan, tilt and zoom features for CCTV cameras may be added to suit operational needs.

Monitoring of cameras may be local or at a remote location, such as the transit control center. Depending on the application, cameras may or may not be recorded.

Modern digital CCTV systems may employ computer-based devices such as IP-enabled cameras, digital video recorders and network video recorders. Computer workstations and servers may be used for control, monitoring or storage of the video images. To ensure the integrity of the system and the images collected, cyber-security must be considered as part of the system design.

CCTV systems are addressed in more detail in the APTA *Recommended Practice* "Selecting Cameras, Recording Systems, High-Speed Networks and Trainlines for CCTV Systems."

Alarm systems

Many control centers have standalone or integrated alarm systems. The alarm systems may include monitoring of intrusion, fire detection, and various other alarm distribution and gathering systems.

2.3.4 Data transmission

Fiber optic networks

Fiber optic networks typically provide the data communications infrastructure between the control center and the various passenger stations, electrical substations and other transit-related buildings and properties.

Copper network

Copper lines are used for short-run local area networks (LANs) that span 300 feet or less from the switch or patch panel to the computer, server or other peripherals. Any spans longer than 300 feet will use a repeater at an interval of less than 300 feet, or fiber optics will be used in place of copper.

Legacy WANs (wide area networks) may use copper lines; however, there is a current trend to phase these out in favor of fiber-optic lines to take advantage of the higher bandwidth.

Leased lines

Leased lines will typically be used for WAN data and/or voice traffic. WAN traffic is any communication outside the immediate facility of the primary or master LAN. Leased lines are used to communicate to outside networks, such as the Internet and other agencies, to bridge child networks to the parent network, or for interconnection of systems where agency-owned cabling is not available. Installation and maintenance of leased lines are typically the responsibility of the telecommunications provider or Internet service provider (ISP).

Wireless

Wireless communication-based systems can be used for applications ranging from local monitoring and control to SCADA and positive train control/communications-based train control (PTC/CBTC) applications. Wireless systems overlay, complement or replace traditional operational-critical infrastructures, such as voice radio, traffic control, automatic equipment identification (AEI), electronic data interchange (EDI), and telephone. Wireless communications allow the use of timely resource status data that can be used with planning and execution tools to process data rapidly for predictive and proactive resource management.

Many types of commercially available "wireless" technologies exist with new versions evolving to satisfy industry-specific applications. The Institute of Electrical and Electronics Engineers' (IEEE) wireless standards include 802.15.4 standard (ZigBee technologies) for monitoring of building automation and control systems; 802.11 (WLAN or Wi-Fi) for wireless local area networking; and 802.16 standard (WiMax technologies) for long-distance broadband wireless access. Other wireless technologies include Bluetooth, proprietary 900 MHz or 2.4 GHz (license-free spread spectrum), fixed-frequency radios (100 to 800 MHz, typically licensed), and cellular GSM/GPRS-based communications.

Wireless is often installed in applications delivering data that are less process critical—i.e., not time critical or deterministic. It is important to note the difference between a deterministic or time-critical application and one that requires only high data reliability/availability. The nature of the radio frequency (RF) environment dictates that there is no guarantee that any given piece of data will successfully be transmitted and received over the air. A well-designed radio network protocol has retry capabilities built in to continue to send that piece of information until it is successfully received, followed by integrity checking in to ensure that transmitted, fragmented data is reassembled at the destination. It is, therefore, quite possible to send important data over a wireless link, as long as the entire system can tolerate some amount of latency. The amount of latency depends on the wireless technology being deployed, as well as the resulting network topology.

"Flat" wireless networks (one type of technology plant-wide) do not lend themselves well to industrial environments with many types of data. Nested sub-network architectures (multiple technologies working together) provide a much higher level of functionality and security, as the RF characteristics of each technology can be appropriately matched with the application layer.

An upcoming use of wireless is communications-based train control.

Wireless networks are found in the following transit systems:

- traffic management;
- yard management;
- crew management;
- vehicle management;
- vehicle maintenance;
- positive train control;
- traffic control;
- mobile node (vehicle intelligence platform [future]);
- remote railway switch control;
- main line work orders;
- wayside maintenance;
- on-track maintenance;
- intermodal operations;
- threat management; and
- passenger services.

2.3.5 Fare collection systems

Fare collection systems used in transit agencies include the integration and control of fare-related equipment such as entry/exit gates, handicapped-accessible gates, emergency gates, ticket vending machines, ticket office machines, parking machines, fare boxes, automated passenger counters, fare validators, ticket encoding machines, stations/garages, systems computers and other networking equipment dealing with fares.

Since fare collection systems frequently are linked to financial systems and institutions such as banks, credit card companies and the back-office function of the transit agencies, the fare collection systems are strictly governed by financial standards, regulations and standards (including PCI and CFMS, just to name a few). They may or not be on a separate network and always require appropriate security controls, which are covered in detail in Part 2 of this *Recommended Practice.*

Fare collection systems are used by transit agencies to help them manage their ridership counts and collect revenue more efficiently at every train station or bus stop. Some fare collection systems are interfaced with both the GPS and radio systems on board buses to accurately determine transaction location and report failure and intrusion of the system in real time.

Payment methods used by fare collection systems may be cash, tokens, magnetic tickets, smart cards, etc.

2.3.6 Vehicle monitoring systems

Vehicle monitoring systems related to rail transit would normally be included under train control systems, above, whereas this category includes automatic vehicle monitoring (AVM) or surface systems, particularly buses, streetcars or nonrevenue equipment.

2.4 Functional description

This section provides a brief description of the systems commonly found in a transit environment. The functionality of these may be included in the systems listed above in Section 2.3, or may be provided by dedicated standalone systems.

2.4.1 Automatic vehicle location (AVL)

AVL is a method to determine the geographic location of a vehicle, usually buses, and relay this information to a central computer system. Most commonly, the location is determined using GPS, and the transmission mechanism is a satellite, terrestrial radio or cellular connection back to a centralized computer system.

2.4.2 Train control systems (TCS)

TCS provide automatic train supervision (ATS) and may include control capabilities to the control center. Train control systems may also provide ATP and ATO for train safety, control of train movements and directing train operations on the main line and in the yards.

2.4.3 Traction power control

Traction power control is normally provided through the SCADA system. Functionality typically includes the monitoring and control of equipment in the electrical substations and along the rapid transit right-of-way. Traction power substations are controlled and monitored from a central location

Some traction power control systems are described below, to illustrate the range of the technology used.

- **Early traction power SCADA systems** were based on hardwired, software-less type legacy systems. A master terminal unit (MTU) is located in the central location with its corresponding remote terminal unit (RTU) at each zone control room in a power substation, which controls and

monitors the substation and circuit breaker house (CBH) equipment. The communication for the MTU/RTU pair is done through point-to-point modems.

- **The next generation of SCADA systems** was microprocessor based, incorporating MTU/RTU architecture as described above. With these systems, a server/client based computer system was also installed as a backup to the MTU panels. The communication for the MTU/RTU pairs is done through point-to-point modems.
- **The typical traction power SCADA system design in recent years** is PLC based with either point-to-point modems or IP-based connectivity through a fiber optic (FO) system. The head-end at the central site is all software based in a fault-tolerant server/client configuration.

2.4.4 Emergency ventilation control

Typically ventilation control is provided by the SCADA system. Functionality includes the ability to provide emergency ventilation of the rapid transit tunnels and stations in the event of smoke or other noxious gases. The ventilation control includes the monitoring and operation of fans, dampers, doors and other associated equipment. Control is normally provided both from the transit control center and local panels at each station. More sophisticated systems allow control of adjacent passenger station equipment from any rapid transit station. Generally the local panels are operated by firefighting personnel only.

Typically, emergency tunnel fan plants are controlled from a central location. When the legacy electromechanical-based control systems are rehabilitated, they are usually replaced with modern PLC-based systems. Fan plants may be controlled via the traction power SCADA system for remote monitoring and control functions. Newer fan plants may use FO connectivity with IP-based secured communication systems. These new systems would have the ability to exercise remote monitoring and control functions from multiple remote sites to fulfill a need for a backup system.

2.4.5 Tunnel drainage monitoring

Tunnel drainage pumping equipment is located throughout the rapid transit systems in order to control the water and waste from filling the tunnels and equipment rooms. Some systems provide for automatic pump control at each location, providing alarms to the control center operators when pump failures occur. Other systems include PLC control systems that control the operation of the pumps providing operators with the ability to control the pump operation via the control center.

Many pump controllers with limited remote alarm monitoring capabilities are still based on hardwired electromechanical relays. Typically when a pumping facility is rehabilitated, modern PLC-based systems are used for local as well as remote monitoring and diagnostic functions. Remote communications might be through dial-up or point-to-point modems. Newer pumping location being built may use FO connectivity with IP-based secured systems for communication with remote sites.

2.4.6 Intrusion/access control (IAC)

IAC is provided to the control center users in order to control and/or monitor access to the transit system facilities. Locations are monitored in order to restrict access to all areas of the rapid transit system, including equipment rooms, emergency exits and the rapid transit wayside.

Intrusion/access control systems may include CCTV equipment, perimeter detection equipment, card access systems, etc. The loss of these systems would weaken the physical security and increase the risk of a physical attack on the transit agency.

CCTV may be used for IAC, platform edge monitoring, crowd control and passenger identification.

Security systems include intrusion-monitoring devices that detect unauthorized access to transit facilities and CCTV for viewing and monitoring selected locations. CCTV may, at times, incorporate computer-based tools that can automatically recognize changes in a scene, or station overcrowding. Such tools are known as artificial intelligence programs. In coordination with the CCTV system, an IAC system is provided to support monitoring and control of non-public facilities and rooms.

Modern IAC systems may use a combination of IP-based communications and security-specific protocols.

2.4.7 Public address

Public address systems are installed in the transit system to provide customer information and emergency evacuation instructions. These systems provide a means of making audible and visual announcements to selected areas in a station, stationwide or to several stations, from the control center or local security room.

2.4.8 Intercom

Intercom systems are installed to provide passenger assistance, as well as emergency response in remote or isolated locations.

2.4.9 Fire detection

Fire-detection systems are installed in various locations of the rapid transit system. Monitoring of the fire-detection system is provided in the control center to be able to determine the location of an emergency situation and to provide quick response.

2.4.10 Seismic monitoring

Seismic detection provides event detection alarms in order to alert for seismic activity.

2.4.11 Gas and pathogen monitoring

Gas monitoring systems include sensors for monitoring gases and other noxious substances in the air and are generally used in bus garages, tunnels or possible confined areas that require ventilation systems. Biological pathogen monitors are also used.

2.4.12 Elevating devices monitoring

This would include systems used for the purpose of monitoring elevators, escalators and other people movers located in the transit stations and used by the general public. The purpose of the systems is to monitor the correct operation of the elevating devices and to report failures to maintenance personnel. Failure of an escalator or elevator may result in overcrowding of stations, a reduction in egress capacity and the inability to move people with disabilities.

2.4.13 Fare collection

Fare collection systems include the integration and control of fare-related equipment, including items like ticket vending machines, fare validators, and other station networking equipment dealing with fares.

2.4.14 Radio systems

Surface radio

Surface radio systems are used to communicate above ground with maintenance vehicles and other nonrevenue vehicles.

Surface vehicle radio system

The surface vehicle radio system is used to communicate between the vehicle operators and the control center. Many transit systems use these systems for both voice and data for use with the AVM system or fleet management.

Subway radio

Subway radio systems are used to communicate to vehicles and personnel below ground and are usually VHF or UHF conventional radio systems that utilize radiating antenna cable in stations and tunnels. Outdoor areas use traditional antennas. Cab-mounted mobile radios are installed in the vehicles, and operating and maintenance staff will carry portable radios. Maintenance and emergency agencies may have some point-to-point channels.

Emergency services radio systems

Emergency systems radio frequencies, (police, fire, etc.) may be retransmitted by the agency's equipment to below-ground areas such as tunnels and other buildings. This system may be separate from the agency's radio systems. This system is similar to subway radio systems and would utilize radiating cables underground and traditional antennas outdoors.

2.4.15 HVAC or building management

Building management systems are used to monitor the operation of the heating, ventilation and air conditioning (HVAC) systems. While normally not an integral part of control and communications systems, loss of HVAC systems could result in failure of sensitive electronic equipment due to extreme changes in temperature and/or humidity levels.

2.4.16 Passenger information displays (PIDs)

Electronic signboards compliant with Americans with Disabilities Act (ADA) requirements enables transmission of text messages from the control center to passenger station platforms. Safety and operations-related messages can be displayed to the traveling public. This system may be tied to other systems, such as the automated train control system, thus allowing for real-time train arrival information.

Public address (PA) systems may also provide the riding public with up-to-the-minute train and system information. Normally this would allow real-time voice announcements to be made to all passenger areas from either the local station or remotely from various control and monitoring facilities.

2.4.17 Telephone/telecommunications applications

The telephone service includes emergency, maintenance and administrative telephones, and passenger assistance intercom at passenger stations, waysides and yards. Typically all telephone lines in a control center are recorded on a voice recorder.

2.4.18 Emergency management panel

Installed in underground stations in accordance with fire/life safety criteria, the emergency management panel integrates alarms, telephone, PA, elevator/escalator and ventilation controls in a single console to permit their use as a consolidated command post in event of an emergency in stations and/or tunnels.

2.4.19 Fire protection system monitoring apparatus

Fire alarm systems are typically installed to protect transit facilities. These include office and maintenance facilities, critical equipment rooms, bus depots and areas within passenger stations.

2.4.20 Emergency alarm (blue light) systems

Typically an emergency alarm (EA) station is installed along the right-of-way and at each passenger station platform. The EA station is identified by blue lights at each location and includes a switch for cutting traction power and a telephone for communicating with the control center. Its function is to allow an individual to shut off traction power during an emergency situation along the right-of-way. Traction power is shut off immediately, while at the same time, a code is transmitted to a command center indicating the location of the EA station. The EA system includes a telephone that is used to communicate to the command center the details of the emergency.

2.5 Diagrams and description of generic networks

FIGURE 1

Legacy Standalone System, Closed (Mainly Physical and Administrative)

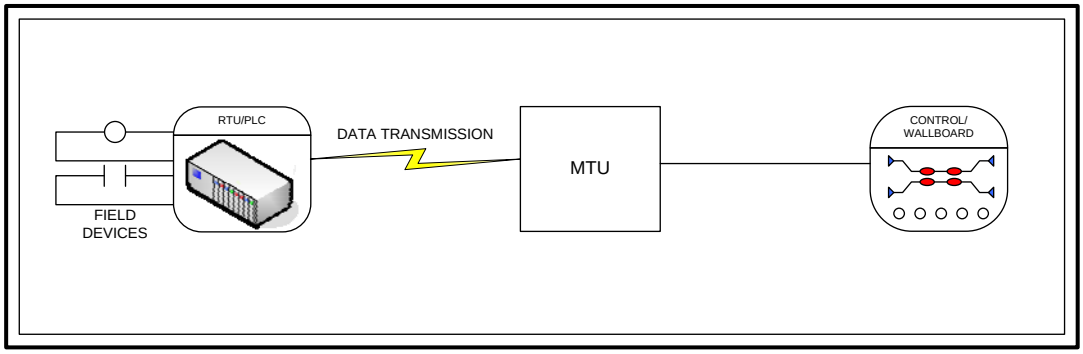


FIGURE 2

Standalone System, (Advanced Technology, Mainly Physical and Administrative with Some Cyber-Security)

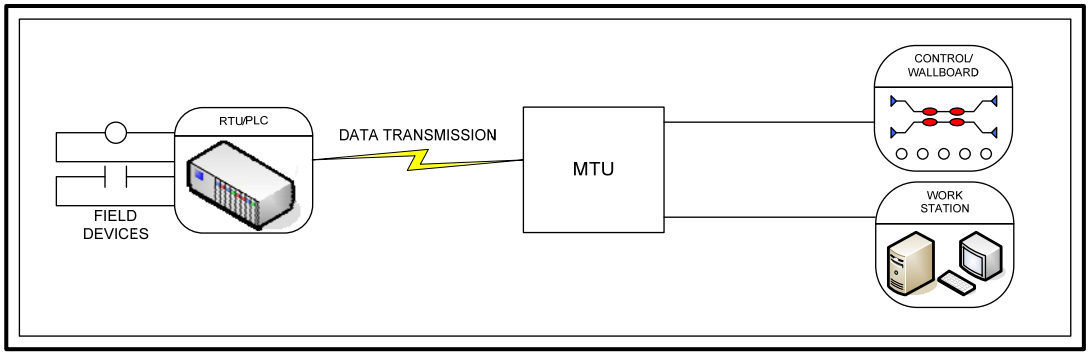


FIGURE 3
Standalone System with Remote Connectivity (Dial-up, Internet Connection, etc.)

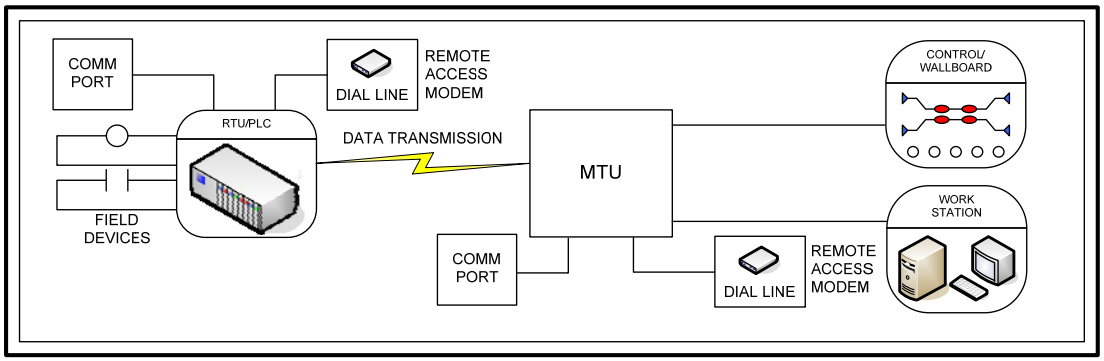
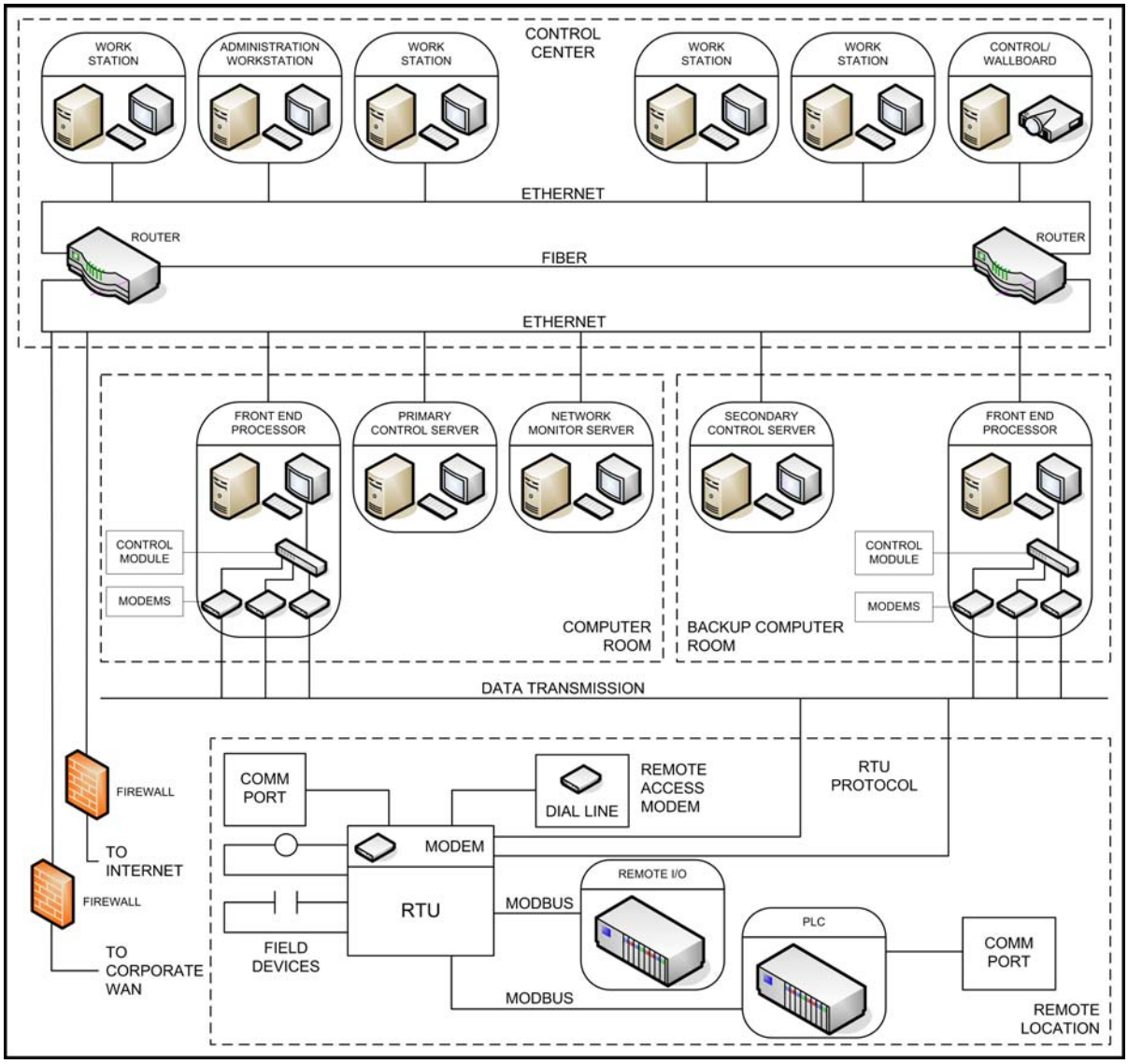


FIGURE 4
Interconnected System (Partially Integrated)



NOTE: The interconnected system includes one primary control server for each application (i.e. SCADA, train control, etc.).

2.5.1 Fully integrated systems

Fully integrated systems are defined as having one common client/server and software architecture interconnected with various field devices and/or interrogating equipment, such as PLCs, RTUs and DDCs. Usually fully integrated systems' server(s) perform load sharing for various applications for control, monitoring and data collection purposes. For example, in a relatively smaller transit agency, remote monitoring, control and data collection of most electrical, mechanical, signals, AVL, etc. systems may be installed and operated on common client/server architecture with appropriate software to perform the intended functions.

Although fully integrated systems may provide some benefits, such as avoidance of duplication of some hardware/software and ease of interoperability among multiple systems, it may pose far more challenges in establishing the criteria for mission-critical to non-mission-critical systems and whether these systems should be interconnected into a single composite system. Depending on transit agency system size, system complexity, organizational culture, multiple operational and maintenance needs and conflicting user requirements, achieving full systems integration may not be practical. Before deploying fully integrated systems, the transit agency should perform detailed studies to determine if fully integrated systems would be a viable approach for its multiple transit systems.

Security access control will still be required at all internal and external interfaces to and from fully integrated systems, similar to what is defined under Section 2.6 and will be covered in Part 2 of this *Recommended Practice*. Since fully integrated systems may serve many users with various applications needs, software accessibility rights and privileges need to be well planned.

2.6 System boundaries and interface to other systems

2.6.1 Local ports for direct connection

Each piece of equipment may have a local maintenance port, generally a COM (serial) or Ethernet port.

2.6.2 Intranet connections

Many systems will connect to the agency's internal business machine network for bidirectional traffic. Usage will be for report generation, display systems and maintenance tasks.

2.6.3 Internet connections

Many systems will have connectivity through the Internet for sharing system information and maintenance connectivity.

2.6.4 Extranet connections

Extranets typically offer external parties with legitimate business needs limited access to some internal systems through an Internet connection. Extranet access may typically be granted to a vendor or an external government agency. Some agencies will require connectivity to other agencies (e.g., police or fire departments) for sharing information such as CCTV, traffic conditions and other center-to-center information sharing.

2.6.5 Modem connections

Systems and equipment may have modem connectivity for dial-up maintenance tasks.

3. Organizing a successful control system security program

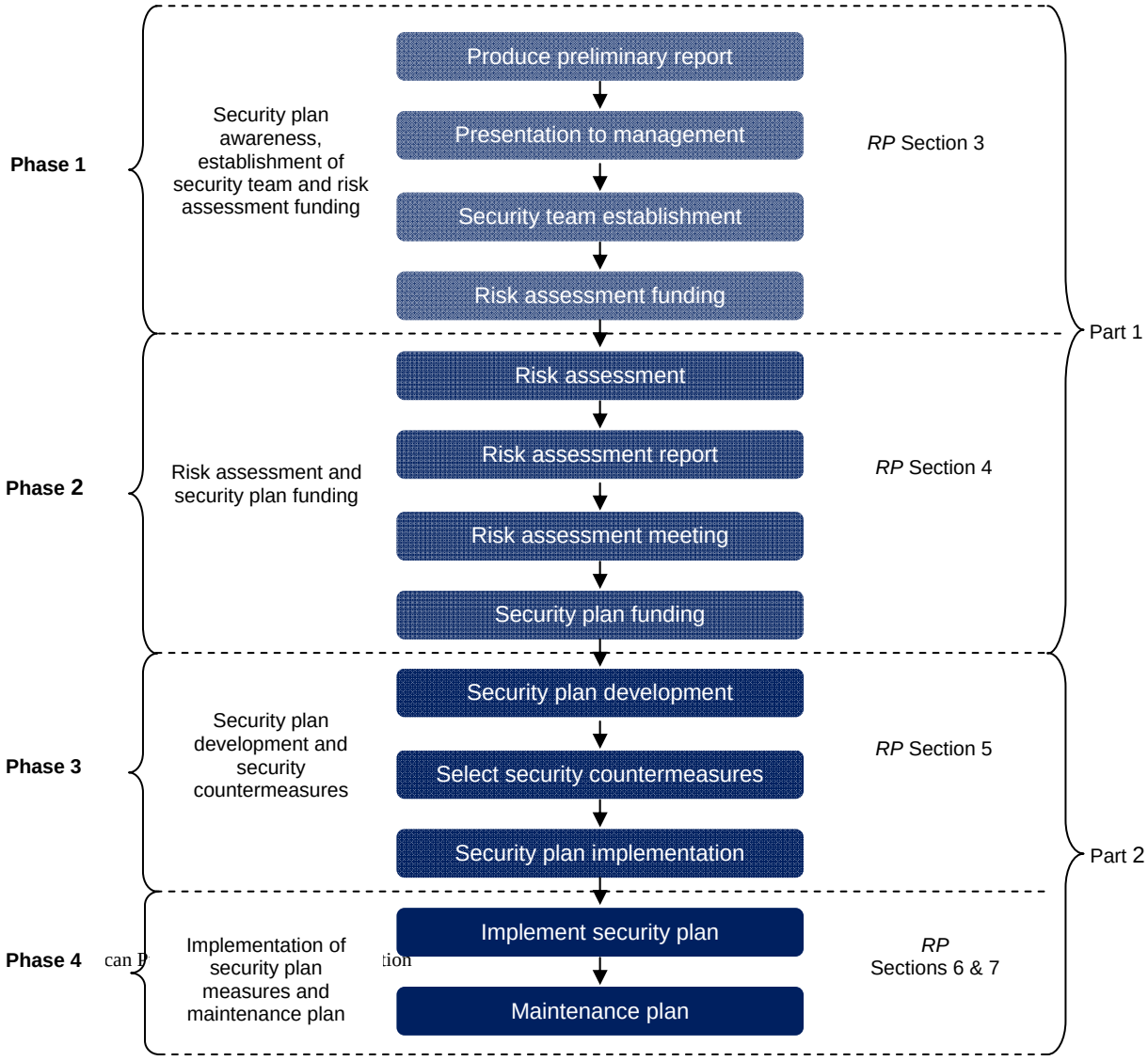
This section is designed to assist transit agencies in the formation and upkeep of a transit control and communications system security program.

History has shown that most agencies do not adequately address control center cyber-security issues, despite the risks identified in Appendix A. Once the agency's senior management is educated as to the importance of the security program, funding can be identified such that an adequate security plan can be developed.

This section lays out a recommended set of tasks the agency should follow in order to ensure that its security program supports its overall business plan. As is identified in this program, support will be required from senior management, system users, maintenance staff (engineers and technicians), other support staff and system and equipment vendors to make the security program successful. The development of the security program is outlined in this section with four main steps of development (see **Figure 5**):

- security program awareness, establishment of security team and risk-assessment funding;
- risk assessment and security plan funding;
- security plan development and security counter measures; and
- implementation of security plan measures and maintenance plan.

FIGURE 5
Security Program



3.1 Phase 1: Security program awareness, establishment of security team and risk assessment funding

The purpose of this section is to ensure that management understands the necessity for security in the transit control systems environment. Appendix A outlines two incidents of security breach that can be used to demonstrate the increasing need for a security program in the transit environment. These two case histories demonstrate the type of vulnerabilities that a transit agency is exposed to when there is no adequate security program in place. The second incident actually occurred at a transit agency where access to the control system was compromised.

It is the responsibility of qualified technical personnel to ensure that management is aware of the effect that an unsecure system will have on the transit system. This involves all levels of concern: life safety, equipment safety, effect on revenue service, customer comfort and satisfaction and other areas that could be affected in the event that the systems are not available.

Agency awareness will include the production of a preliminary report to management, followed up with a formal management presentation with the view of receiving funding for a thorough risk assessment of the control center and related systems and equipment. The first step will be to ensure that the appropriate people in the transit agency are aware of the repercussions if a security program is weak or nonexistent. The second step will be to secure funding for a risk assessment that will identify weaknesses and vulnerabilities in the transit agency infrastructure. When establishing the budget for the risk assessment, a contingency allowance may be added to address issues that could be resolved with minimal effort and expense (i.e., “low-hanging fruit”). The agency must appreciate why a security program is required and start the process to initiate the security program.

In order to make the security program successful, the risk assessment must be extremely thorough. This will necessitate the involvement of all interested parties in the organization. A large organization may require many members from different departments, whereas a smaller organization may include only a few people. Typically those responsible for the following areas will be involved:

- system engineering;
- maintenance;
- IT development;
- system users;
- system safety; and
- transit security.

Representatives from each discipline will be formed into a task group whose responsibility will be to ensure that the risk assessment includes all systems, equipment and physical locations in which equipment is installed.

3.2 Phase 2: Risk assessment and security plan funding

The key to a successful control center security program will be the thoroughness of the risk assessment. The risk assessment will be the focal point of the security program, as it identifies all systems, equipment, data paths, computer operating systems and the physical location of all equipment (therefore cyber and physical aspects of security should be reviewed). The risk assessment will also identify areas of cyber-security, including a review of all system users and required access points to the systems. It should be noted that most agencies will already have some level of risk assessment in place; however, in most cases the existing risk assessment will be general in nature and will not meet the requirements of a control center security program. The risk assessment will be a confidential document.

The risk assessment will analyze the systems in order to determine areas of vulnerability and the likelihood of a loss of functionality resulting from failure of a system component. The failure may be the result of internal system weakness (hardware or software failure) or external influences (physical or cyber attack). The risk assessment will evaluate each single piece of hardware or system link and examine the effect on the system functionality if that component fails. The loss of functionality will then be examined to determine the consequences that will occur to the agency, measured in either loss of money, deterioration of revenue service or loss of life or physical safety of the public or agency personal or equipment. The risk assessment will then provide recommendations that can be used to mitigate the risks. The output of the risk assessment will be used in the development of security plan countermeasures described later in this document. Details of the risk assessment are covered in Section 3.1 and details of risk management are covered in Section 3.2 of this document.

The following is from DHS's "Catalog of Requirements," dated 2008:

> The organization develops, disseminates and periodically reviews/updates:
>
> 1. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
> 2. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
>
> The organization develops a risk management plan. The risk management plan is reviewed and approved by a senior organization official.

3.3 Phase 3: Security plan development and security countermeasures

The development of the security plan will be very detailed and requires time to explore the control and communications systems infrastructure, policies and procedures, and to develop adequate security measures that address recommendations resulting from the risk assessment. The plan will include physical and cyber-security measures for all systems and equipment including existing (legacy) equipment, new system procurement, equipment maintenance and support. Details of the security plan development and countermeasures will be covered in Part 2, Section 5 of this *Recommended Practice*.

A control and communications systems security plan will have to be developed and kept current in order to meet the objectives laid out in this *Recommended Practice*. This control and communications systems security plan will include the following major tasks:

- Control and communications systems boundaries:
  - Identify the systems.
  - Identify the equipment.
  - Identify the locations.
  - Identify the stakeholders.
- Work group:
  - Include all stakeholders.
  - Identify responsibilities of the stakeholders.
- Policies and procedures:
  - administrative
  - technical
  - cyber
  - physical
  - maintenance
- Security measures

- Management reports
- Maintenance issues
- Training

In order to produce an adequate security plan, the agency will have to assign the initial tasks to a particular individual, (probably from the engineering support or IT team). The responsibility of this person will be to "get the ball rolling." This individual would then perform the following tasks:

- Identify initial tasks, stakeholders and policy requirements.
- Produce a management report.
- Form the task group:
    - List stakeholders (IT, engineering, operations & communications).
    - Form the stakeholders into a control security committee.
- Educate the task group members as to the importance of the security plan.

Once the task group has been set up, it will be responsible for the development of the security plan. Key responsibilities will be assigned to each member.

3.4 Phase 4: Implementation of security plan measures and maintenance plan

After the development of the security plan, it is essential that both a security plan management system and a maintenance plan are established. Details of the security plan countermeasures and maintenance plan are covered in Part 2, Sections 6, 7 and 8.

3.4.1 Case histories

Refer to Appendix A for examples of case histories as they apply to transit and other industry sectors.

4. Risk assessment and management

4.1 Risk assessment

The process of risk assessment enables an organization to identify its mission critical processes, assets and functions, which are necessary for the existence and viability of that organization, and rank these assets in the order of criticality. It also assesses the probability/likelihood of risk from threats to these assets and its impact to the business.

The tables in Appendix B may be useful to reference when going through the risk-assessment process as described in this section.

4.1.1 Stages of the risk-assessment process

The following are the major steps in organizing for and conducting a risk assessment for a transit agency:

- Generate management support and empowerment for the risk-assessment process.
- Form the risk-assessment team from technical experts and stakeholders.
- Identify assets and loss impacts.
- Identify threats to assets.
- Identify and analyze vulnerabilities.
- Assess risk and determine priorities for the protection of critical assets.
- Identify countermeasures, their costs and trade-offs.

4.1.2 Generate management support and empowerment for the risk-assessment process

Per Section 3, management support is necessary for the risk-assessment process. The process takes time and commitment, and empowerment and resources for the team are necessary.

The following is from DHS's "Catalog of Requirements," dated 2008:

> The organization obtains senior management support for a cyber security risk assessment process.

4.1.3 Form the risk-assessment team from technical experts and stakeholders

Referring to the complete list of systems noted the "Scope and Purpose" section at the beginning of this document, decide which systems of the transit agency are within the scope of the risk-assessment process. It may be all of the systems, or if this scope is too big, it may be a more manageable subset of these. The areas to be covered will probably be revisited once the team is formed.

The team that is formed should be of a combination of the organizational "owners" of these areas, technical experts from these areas, and auxiliary groups. For instance a team might include Engineering, Operations, Maintenance, HR, Safety, IT, Security, etc.

The following is from DHS's "Catalog of Requirements," dated 2008:

> The organization forms a cross-functional risk assessment team composed of individuals from all of the departments affected by the cyber security program.
>
> **NOTE:** Sections 4.1.4, 4.1.6, 4.1.7 and 4.1.8 have been excerpted from NERC's "Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment."

4.1.4 Identification of assets and loss impacts

- Determine the critical assets that require protection. This may include list of control and computing equipment, physical and network layouts, etc., and may include hard copy drawings, electronic network drawings, database printouts, etc. Keep this information in a secure central location for the team.
- Identify possible undesirable events and their impacts.
- Prioritize the assets based on consequence of loss.

The following is from NIST's "Guide to Industrial Control Systems (ICS) Security," SP800-82, dated September 2008:

> **Availability Requirements.** Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable.
>
> **Risk Management Requirements.** For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns.

4.1.5 Identification of threats to assets

- Identify source of potential threats to critical assets

The following is from NIST's "Risk Management Guide," SP800-30, dated July 2002:

> **Threat:** The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

> **Threat-Source:** Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability
>
> **Common Threat-Sources:**
> Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
>
> Human Threats—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
>
> Environmental Threats—Long-term power failure, pollution, chemicals, liquid leakage.

4.1.6 Identification and analysis of vulnerabilities

- Identify potential vulnerabilities related to specific assets or undesirable events.
- Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.
- Estimate the degree of vulnerability relative to each asset.

The following is from NIST's "Risk Management Guide," SP800-30, dated July 2002:

> **Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

4.1.7 Assessment of risk and the determination of priorities for the protection of critical assets

- Estimate the degree of impact relative to each critical asset.
- Estimate the likelihood of an attack by a potential threat. Likelihood is the probability that a particular vulnerability may be exploited by a potential threat (derived from NIST Risk Management Guide 800-53).
- Estimate the likelihood that a specific vulnerability will be exploited. This can be based on factors such as prior history or attacks on similar assets, intelligence, and warning from law enforcement agencies, consultant advice, the company's own judgment, and additional factors.
- Prioritize risks based on an integrated assessment.

The following is from DHS's "Catalog of Requirements," dated 2008:

> The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood." Risk is assessed across the organization by determining the likelihood of potential threats and cost if the threat is realized.

4.1.8 Identification of countermeasures, their costs and trade-offs

- Identify potential countermeasures to reduce the vulnerabilities.
- Estimate the cost of the countermeasures.
- Conduct a cost-benefit and trade-off analysis.
- Prioritize options and recommendations for senior management.

4.2 Formulating a risk management strategy

In Section 4.1, the risk assessment process shows which portions of the control and communications networks are high risk, medium risk and low risk. The transit agency may assign its own significance to these relative risk levels. An example explanation of high, medium and low risk level significance from NIST 800-30 is given in Appendix B.

Recommendations are made to management in a risk-assessment report that includes any security controls or countermeasures to mitigate risks.

The risk assessment committee then confers with upper management at the transit agency, and moves into risk management mode. The team, together with management, looks at the risk picture portrayed by the assessment output, and asks the following questions:

- Which risks can I accept?
- Which risks may I transfer (by taking out insurance, for instance)?
- Which risks are unacceptably high and should be reduced? For instance, a severe-consequences event with medium likelihood may prove to be unacceptable. For these risks, countermeasures or security controls, applied within the context of creating a security plan, are applied to bring the risk level down to an acceptable level.

Part 2, Section 5, will describe the process of creating a security plan, according to the security program discussed in Section 3. A security plan is the framework for administrative, physical and technical controls.

The risk team confers with upper management at the transit agency, looks at the magnitude of the risks and the potential consequences, and upper management allocates the size of the total budget available to dedicate towards the security management system and its controls. This budget would cover man hours, equipment expenditures and security maintenance.

Expenditures for security controls are then allocated in view of the risk assessment to bring high risks down to an acceptable level. The result that is desired from the risk management stage is a balance where the total risk picture is moderated by applying the available security control resources, leaving a balanced protection from risks. The expenditure allocation method or formula will vary with each transit agency.

4.3 Additional information

Additional information is available from the following sources:

- National Institute of Standards and Technology, “Risk Management Guide for Information Technology Systems,” NIST SP800-30. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- National Institute of Standards and Technology, “Guide to Industrial Control Systems (ICS) Security,” NIST SP800-82. http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf
- North American Electric Reliability Council (NERC), “Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment,” 1.0. http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf

Preview of Part 2

This section gives a preview of the material included in Part 2 of this *Recommended Practice*.

As mentioned in the Introduction, Part 1 guides a transit agency through the formation of a control and communications security program, and up through the risk assessment/risk management step.

Section 5, "Applying security controls (countermeasures) to mitigate risks," addresses the following subjects:

- Developing the security plan
- Administrative security (including policy and procedures and personnel security)
- Physical and environmental security
- Technical security controls (countermeasures)
    - Design stage controls
    - Technology (including filtering and blocking, intrusion detection, malware, encryption and verification)
- Applying technical security controls to generic network drawings from Section 2

Section 6, "Execution of a security plan," includes the following subjects:

- Role of a project management perspective in executing a security plan
- Prove-in and phase-in of security controls (countermeasures)
- Moving into the maintenance phase of the security plan

Section 7, "Maintaining a security plan," includes the following subjects:

- Incident response, investigation and mitigation
- Security audits
- Maintenance phase of a security plan

Section 8, "Continuity of operations/disaster recovery," includes the following subjects:

- Continuity of operations planning
- Overview of disaster recovery:
    - Writing the recovery plan
    - Organizing disaster recovery teams
    - Recovery procedures
    - Command centers
    - Information directory requirements

Appendix A: Cyber attack news stories and case studies

The following news stories and case studies from transit and other industries illustrate the consequences of cyber attacks.

CSX railway virus attack

In 2003, the "Sobig virus" struck CSX's Jacksonville, Florida, headquarters, bringing down signaling, dispatch and other related systems. Details may be found in the following web news account: http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml

Amtrak trains operating in CSX's territory were also affected. Trains were delayed from between four to six hours.

Another web news account related that the virus struck at 1:15 in the morning, and most affected computers were fixed by 7:15 a.m. However CSX had said it would take up to 24 hours to completely recover. Consequences were losses from the freight and passenger delays, as well as confusion and extra computer cleanup from the virus.

Polish tram hack

In 2007, a 14-year-old Polish teenager in the city of Lodz studied the tram and track operations in his city and built a device similar to a TV remote control to change switch points on the tracks. Twelve people were sent to the hospital with injuries and four vehicles were derailed. The details may be found in this web news account: http://www.theregister.co.uk/2008/01/11/tram_hack/

This report raises the question: If this is what a 14-year-old can do, what can a disciplined team of hackers do?

Computer worm in nuclear plant control room

The U.S. Nuclear Regulatory Commission (NRC) in August 2003 issued an alert to all nuclear plant operators about a situation occurring earlier that year at the Davis-Besse plant in Ohio. The "Slammer" computer worm entered the plant control systems by a circuitous route through a T-1 communications line.

The worm was able to reach and take down the "Safety Parameter Display System," which is a system that displays the status of critical reactor monitoring sensors such as core temperature, pressure, etc. Fortunately the plant was off-line at the time, and a backup analog system was able to take over.

The event is described at this URL: http://www.theregister.co.uk/2003/09/03/us_warns_nuke_plants/

Appendix B: Supplementary information from NIST documents

Table A3-1. Summary of IT System and ICS Differences

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable Delay and/or jitter is not acceptable
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for operations	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities

Table A3-1. Summary of IT System and ICS Differences

Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

Source: NIST 800-82, pages 3-3, 3-4. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Table A3-2. Adversarial Threats to ICS

Threat Agent	**Description**
Attackers	Attackers break into networks for the thrill of the challenge or for bragging rights in the attacker community. While remote cracking once required a fair amount of skill or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. Many attackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of attackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Bot-network operators	Bot-network operators are attackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of compromised systems and networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or the use of servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the U.S. through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop attacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power–impacts that could affect the daily lives of U.S. citizens.

Table A3-2. Adversarial Threats to ICS

Insiders	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners. Inadequate policies, procedures, and testing can, and have led to ICS impacts. Impacts have ranged from trivial to significant damage to the ICS and field devices. Unintentional impacts from insiders are some of the highest probability occurrences.
Phishers	Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (e.g., DoS).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information. Terrorists may attack one target to divert attention or resources from other targets.
Industrial spies	Industrial espionage seeks to acquire intellectual property and know-how by clandestine methods

Source: NIST 800-82, pages 3-5, 3-6. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Table 3-7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Source: NIST 800-30, page 25. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

References

International Society of Automation, "Security for Industrial Automation and Control Systems: Part 1: Concepts, Terminology, and Models," ANSI/ISA Standard 99.00.01, 2007.

International Society of Automation, "Security for Industrial Automation and Control Systems: Part 2: Integrating Security into the Manufacturing and Control Systems Environment," ANSI/ISA Standard 99.00.02, 2007.

International Society of Automation, "Security Technologies for Industrial Automation and Control Systems," ANSI/ISA Technical Report TR99.00.01, 2007.

North American Electric Reliability Council (NERC), "Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment," Version 1.0, June 2002. http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf

North American Electric Reliability Council (NERC), "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations," December 2006. http://www.us-cert.gov/control_systems/pdf/2007_Top_10_Formatted_12-07-06.pdf

National Institute of Standards and Technology (NIST), "Guide to Industrial Control Systems (ICS) Security," final public draft, 2008. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

National Institute of Standards and Technology (NIST), "Risk Management Guide for Information Technology Systems," SP800-30, July 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

The President's Critical Infrastructure Protection Board, U.S. Department of Energy, "21 Steps to Improve Cyber Security of SCADA Networks," http://www.oe.energy.gov/DocumentsandMedia/21_Steps_-_SCADA.pdf

U.S. Department of Homeland Security (DHS), "Catalog of Control Systems Security: Recommendations for Standards Developers," September 2009. http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

U.S. Department of Homeland Security National Cyber Security Division, "Control Systems Cyber Security: Defense in Depth Strategies, May 2006. http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

Definitions

automatic train operation (ATO). On-board train system supporting driverless or driver assist operations.

automatic train protection (ATP). On-board train safety system to apply brakes if signal missed by operator.

automatic train regulation (ATR). Typically off-board train; supporting safe and efficient train movements via interface with ATO.

automatic train supervision (ATS). Advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.

channel banks. Typically used to multiplex many channels of analog voice, video, audio and serial communication devices across a FOCTS.

core switch. A fault-tolerant Ethernet routing switch.

crossing systems. Grade crossing protection systems.

CSU/DSU. Typically used to bridge digital data (e.g., Ethernet) across other digital mediums (e.g., T1).

centralized train control (CTC). Typically supporting only basic automatic routing (also known as dispatch systems).

countermeasures. Security controls to reduce risk of attack or mitigate consequences.

device networks/Fieldbus networks. Intelligent I/O comms: Profi-bus, CAN, ControlNet, etc.

device server. Similar to a terminal server that contains custom software typically used for protocol conversions.

edge switch. Local area Ethernet routing switch.

event recorder. A device used locally in signal bungalows to record signal system related events.

Extranet. Private network to share business information with suppliers and other businesses.

fiber optic modem (FOM). Typically used for serial communication devices that need to communicate through electrically noisy environments.

gas monitoring. Air quality measuring devices.

hub. Ethernet device to connect Ethernet devices. Non-switched and typically non-managed.

Internet. Worldwide public network to exchange data using IP.

Intranet. Private organizational network to communicate data shielded from public Internet.

isolated system. A system that has no connection to neighboring systems, and may be considered secure from external network based cyber attack.

modem. A device used to transmit digital data across analog mediums.

radio. An above-ground or tunnel method to communicate voice and data wirelessly.

router. A device to segment networks.

seismic detection. Alarms to alert for seismic activity.

terminal server. A device to aggregate serial communication channels (e.g., RS-232) onto an IP-based Ethernet network.

transit. A term that encompasses all mass transportation system types, such as light rail, heavy/metro rail, commuter rail, regional rail, inter-city/mainline rail, bus, bus rapid transit, etc.

vital. A term applied within rail safety control systems to denote fail-safe operation. (Derived from IEEE Std 1483, 2000 glossary, "vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.")

vehicle tag (VTAG). Identification systems (typically train-to-wayside loops)

web. Synonymous to World Wide Web browser-based applications.

Wi-Fi. 802.11a-n wireless local area networks.

WiMax. A wireless digital communications system, also known as IEEE 802.16, that is intended for wireless metropolitan area networks.

Abbreviations and acronyms

ACS	access control system
ADA	Americans with Disabilities Act
AEI	automatic equipment identification
APTA	American Public Transportation Association
ARO	annual rate of occurrence
ATO	automatic train operation
ATP	automatic train protection
ATR	automatic train regulation
ATS	automatic train supervision
AVL	automatic vehicle location
AVM	automatic vehicle monitoring
CACF	central alarm and control facility
CAD	computer-aided dispatch
CBH	circuit-breaker house
CBTC	communications-based train control
CC	central control
CCS	central control system
CCTV	closed-circuit television
CDMA	code division multiple access
CFMS	Contactless Fare Media System Standard
CFR	Code of Federal Regulations
CIS	customer information system
COR	(DHS) Central Office of Record
COTS	commercial off-the-shelf
CSU/DSU	channel service unit/data service unit
CTC	centralized train control
DDC	direct digital controls
DHS	U.S. Department of Homeland Security
DVR/NVR	digital video recorder/network video recorder
EA	emergency alarm
EMC	electromagnetic compatibility
ETEL	emergency telephone
F&I	fire and intrusion

FAS	fire alarm system
FO	fiber optics
FOM	fiber optic modem
FRA	Federal Railroad Administration
GHz	gigahertz
GPRS	general packet radio service
GSM	Global System for Mobile Communications
HR	human resources
HVAC	heating, ventilation and air conditioning
I/O	input/output
IAC	intrusion/access control (physical)
ID	identification
IDS	intrusion detection system (network)
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet protocol
ISA	International Society of Automation
ISP	Internet service provider
IT	information technology
LAN	local area network
LRT	light rail transit
MAN	metropolitan area network
MHz	megahertz
MTU	master terminal unit
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Council
NIST	National Institute of Standards and Technology
NMS	network management system
NRC	Nuclear Regulatory Commission
OCC	operations and control center
OCS	overhead contact (catenary) system
PA	public address
PBX	private branch exchange
PCSRF	Process Control Security Requirements Forum
PCI	payment card industry
PIDS	passenger information display signs
PLC	programmable logic controller
PTC	positive train control
PTEL	passenger assistance telephone
RF	radio frequency
RTU	remote terminal unit
SCADA	system control and data acquisition
SCS	supervisory control system
SMU	signal monitoring unit
SNL	Sandia National Laboratories
SOHO	small office/home office
TCS	train control system
TPSS	traction power sub-station
TVS	tunnel ventilation system
TWC	train-to-wayside communications
UTFS	Universal Transit Fare System Task Force

VLAN virtual local area network
VMB variable message board
VMS variable message sign
VoIP voice over IP
VPN virtual private network
VTAG vehicle tag
WAN wide area network
WLAN wireless local area network